NCPROTECT™

DYNAMIC DATA DISCOVERY, CLASSIFICATION & SECURITY FOR NUTANIX FILES

NUTANIX READY • AHV •

Executive Summary

NC Protect™ for Nutanix Files dynamically adjusts file protection based on real-time analysis of file content and comparison of user and file context to ensure that users view, use and share files according to your business regulations and policies.

NC Protect applies security and encryption to Nutanix Files content without the overhead of manually administered folder shares and permissions. Data can be automatically classified and encrypted based on the content sensitivity and metadata associated with the file. Organizations no longer need to rely on complex folder hierarchies to control access, instead they can easily ensure their sensitive data is appropriately protected at the file level.

Key Benefits

- Automatically discover, classify, and restrict access to or encrypt files based on the presence of sensitive data including PII, PHI, IP and other factors.
- Limit access and apply protection at the file-level using secure metadata.
- Control who can access files and how they can use and share them.
- Monitor and audit file access against regulatory and corporate policies.
- Detect potential violations and initiate workflows and notifications to mitigate risk.
- Audit trails and forensics track access to sensitive data to ensure transparency and accountability.

FILE SHARE DATA POSES A SIGNIFICANT RISK

Organizations rely on file storage platforms like Nutanix Files to store and collaborate on unstructured content. And that content is growing quickly. According to IDC 80 percent of worldwide data will be unstructured by 2025. As the amount of unstructured data grows, so does the risk to your business. The 2019 Insider Threat Report reported 39% of respondents identified cloud storage and file sharing apps as the most vulnerable to insider attacks. This presents a major challenge for IT and IS teams looking to ensure data security and compliance.

DYNAMIC DATA DISCOVERY, CLASSIFICATION & SECURITY FOR NUTANIX FILES

Nucleus Cyber provides Nutanix Files users with intelligent data-centric security for secure collaboration without the complexity. The NC Protect solution dynamically controls access to business-critical content and restricts how authorized users can share it and with whom, based on real-time comparison of user context and file content to enforce data governance and security policies. NC Protect provides unmatched information protection capabilities to prevent accidental sharing, data misuse and loss, while maintaining a simple and intuitive user experience that empowers customers to start securing information in hours, not days or weeks.

DYNAMIC, GRANULAR INFORMATION PROTECTION WITHOUT THE COMPLEXITY

Discover and Classify Data

NC Protect's policy manager features hundreds of pre-defined checkpoints for US and international privacy policies (Privacy Acts, GLBA, COPPA), and other regulatory mandates including HIPAA, FISMA, PCI DSS and more. Easily define and configure custom checkpoints to match your organization's unique privacy, confidentiality and security policies.

Control Access and Sharing

NC Protect leverages dynamic access, usage denial rules and a secure viewer to ensure that only approved users can access and share your business content based on the file's classification and the user's current location, device, and security clearance. It can automatically encrypt data when it leaves the safety of the corporate file system. It also audits access to sensitive data and provides reports on compliance violations to stakeholders, ensuring transparency and accountability.

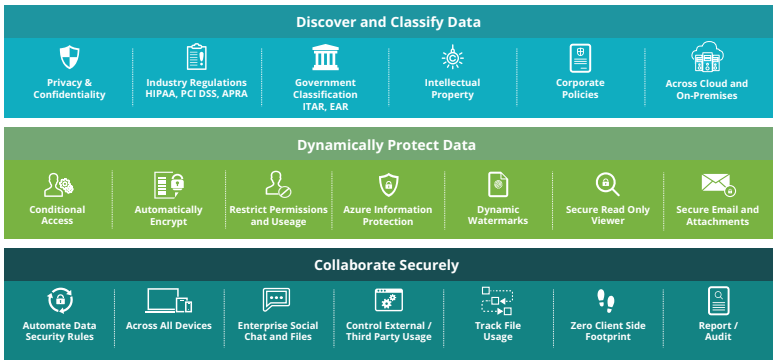
Reduces Complexity for Faster Results

NC Protect's intuitive user experience empowers users to start securing information in hours, not days or weeks. It is Nutanix Ready and requires no additional client-side application simplifying deployment and reducing the time that your content is at risk.

DYNAMICALLY SECURE NUTANIX FILES AT THE DOCUMENT LEVEL

NC Protect uses metadata-driven, item level security to restrict access to, encrypt, track and prevent unauthorized sharing of content based upon the presence of sensitive and/or non-compliant information, offering content-aware data loss protection (DLP) capabilities for Nutanix Files.

Organizations using Nutanix Files in addition to Microsoft 365 or SharePoint on-premises for file storage and collaboration can leverage NC Protect's rules across all of these platforms to centrally manage policies, classifications and controls.



DISCOVER

Locate all sensitive and confidential data (PII, PHI, HR, IP, etc.) to create an 'information footprint' of your sensitive data using a single set of rules for one or multiple on-premises and cloud environments.

CLASSIFY

Once sensitive information is detected the file can be automatically classified based on the sensitivity of the content and pre-defined governance policies. You can also define which users can classify or reclassify data, unlike standard metadata that can be modified by anyone that has document access.

RESTRICT ACCESS

Based upon the business rules associated with its classification, access to a file can be restricted to a specific individual or group, even if a wider audience has access to the rest of the folder where the item physically resides. With file level controls, users and administrators can reduce the number of folders needed to enable secure collaboration with a subset of authorized users. Managing access down to the file level is made possible by leveraging the data and user attributes rather than the data location.

ENCRYPT

Data loss prevention is a critical issue for many organizations. In addition to securing a document based on its classification (metadata), NC Protect can further secure Nutanix Files content by encrypting it. This means only properly credentialed users will be able to read the content – whether inside or outside of the file share – even if they have administrator privileges, making it safe to store confidential documents such as Board and HR documents. It also ensures any documents that make it out of the file system can only be accessed by the credentialed users.

PREVENT SHARING & MISUSE

To further extend the tracking process you can also define rules in NC Protect to prevent the distribution of sensitive information or confidential documents to minimize the risk of data loss. For example, if a file is added to a folder and member does not have proper access to that category of document, then the file can be hidden from the view of the unauthorized individual. Users can also be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs.

MITIGATE RISK

Using workflows and native integration with SIEM tools such as Splunk, NC Protect can trigger access approval requests for policy officers or managers or to request justifications from users. Complete business rules can be developed so that you can remediate compliance issues and task the proper individual(s) in the organization to review and potentially classify, alter the classification of, or encrypt the content.

AUDIT & REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. It reports on the number of issues identified by classification level and allows policy officers to review the results and rescan, reclassify or reapply permissions if needed. The list can be filtered based on flexible search conditions and exported to various formats for reporting or archiving purposes.

NUTANIX READY • AHV •

ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED ACCESS AND CONTROL

archTIS' granular data-centric approach to security enforces a zero trust methodology through conditional, attribute-based access control (ABAC) at the item-level. Since access and information protection are applied to individual files, chats and messages, as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated on from any Nutnix Fles folder. NC Protect ensures access to the file is restricted to only those who have permissions to it as defined by its classification.

archTIS

archTIS.com | info@archtis.com Australia | United States | United Kingdom